40

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,230	09/05/2000	Chung Nan Chang	2170	7762

7590 03/29/2005

Donald E Schreiber
Donald E. Schreiber A Professional Corp.
Post Office Box 2926
Kings Beach, CA 96143-2926

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/655,230	**Applicant(s)** CHANG, CHUNG NAN	
	Examiner Jung W Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 28 January 2005.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-41 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-41 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

1. Claims 1-41 have been examined.

Response to Arguments

2. The following is a response to applicant's arguments presented on pgs. 3-29 in the amendment filed on January 28, 2005 ("Remarks").

3. Applicant's arguments, see pg. 3, with respect to the objection to the Abstract, have been fully considered and are persuasive. The objection to the length of the Abstract has been withdrawn.

4. Applicant argues that the Crandall prior art does not cover the limitations as recited in applicant's claim 40, specifically,

> *... as best summarized in the table attached hereto as Exhibit B and as explained in greater detail above, with respect to the text of independent claim 40 the Crandall '616 fails to disclose or to suggest:*
>
> *1. that the "sender 1201" stores <u>a plurality of public quantities</u> into the "public source 813" which the "receiver 1202" retrieves during digital signature authentication;*
>
> *2. at least <u>two (2) expressions are evaluated</u> by the receiver <u>using a plurality of public quantities</u>; and*
>
> *3. comparing <u>the at least two (2) expressions evaluated using a plurality of public quantities</u>.* Remarks, pg. 17, last paragraph-pg. 18, first paragraph.

5. It is noted in the original rejection of claim 40 (Office action dated August 11, 2004) and the rejection presented in the instant action, the claim has been found to be anticipated by Crandall '616' in light of Figures 8-12, the Abstract, col. 1:50-56 and 20:43-60); applicant's traversal in the Remarks and Exhibit B only discusses Crandall in terms of 1:50-56 and Figure 12 and related text (Remarks, pgs 8-9; Exhibit B), and does not address Figures 8-11 and related text.

6. In light of figures 8-12 of Crandall, Examiner respectfully disagrees with applicant's argument and reiterates that Crandall does teach all limitations of claim 40.

7. Regarding the limitation of [1.] a sender storing a plurality of public quantities into the public source, which the receiver retrieves during digital signature authentication, figure 8 of Crandall identifies a public source (Reference No. 813) storing a plurality of public quantities for digital signature authentication. Crandall discloses the context of this public source as:

> *a separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 801 and receiver 802, the initial point (x1,y1), the field Fpk, and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may transmitted [sic] between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 801 through line 815 and to receiver 802 through line 814.* [emphasis added] col. 12:63-13:4.

8. Hence, in the context of figure 8, the public keys, the initial point, the field, and the curve parameter are the plurality of public quantities stored (published), then used

by the receiver to generate a mutual one-time pad to authenticate a digital signature signed by the sender. Crandall, 14:20-39. By virtue of the fact that the public source is defined only as a repository for public quantities, and the sender must share it's cryptographic context (sender's public key and context values (x1, y1), the Field Fpk, and curve parameter "a") with the receiver for proper generation of the one time pad, it is implicit in the disclosure that the plurality of public quantities is stored by the sender. This feature is further established in Figure 3, reference no. 303 and 16:4-9.

9. Moreover, in figure 11, Crandall expressly teaches [2.] at least two expressions being evaluated by the receiver using a plurality of public quantities, [3.] and comparing the at least two expressions evaluated using a plurality of public quantities: reference no. 1105 identifies two expressions (e=x and f=x) using a curve parameterized by public quantities "a", a field Fpk and initial point (X1/1), and the sender's public key; wherein only when e=x and f=x is the signature determined to be valid. Hence, Crandall teaches and/or suggests all limitations of claim 40.

10. In reply to applicant's argument that Hellman does not teach all the limitations of claim 27, specifically *Hellman, et al. patent fails to disclose or to suggest either sub-element "i" or sub-element "ii" of element "b. ports" in the body of independent claim 27* (Remarks, pg. 20, 1st paragraph), examiner respectfully disagrees.

11. The premise of applicant's argument that Hellman does not disclose sub-element "ii" of element "b.ports" is based on a reading of Hellman wherein reference no. 12 is the transmitter (sender of the ciphertext) and reference no. 11 is the receiver (decrypter of

the ciphertext) in figure 1. (Remarks, pg 20, 1st full paragraph-pg. 21) This is not a valid interpretation: Hellman explicitly defines converser 12 as the receiver of the ciphertext and converser 11 as the sender of the ciphertext. Hellman, 3:40-69. Hence, contrary to applicant's conclusion that "the sending converser 12 transmits only a single quantity Y2 to the receiving converser 11" (Remarks, pg. 21), Figure 1, clearly shows quantities "q", "a" and "Y1" as being transmitted from the sender (converser 11) to the receiver (converser 12).

12. Applicant's argument that sub-element "i" of element "b.ports" is not taught is also based on the same inadequate premise. (Remarks, pgs 22- 24) Moreover, applicant's argument assumes the plurality of public quantities and the sender's quantities are mutually exclusive; however, this is not defined in the claims, and hence is not a necessary limitation to show obviousness.

13. Moreover, applicant's definition of Y1 or Y2 being a single quantity takes a narrow definition of the terms used by Hellman. For example Hellman discloses:

> *Signal Y1 may be generated to represent the number obtained by raising the number represented by signal to the power represented by signal X1, modulo the number represented by signal q; this transformation may be represented symbolically as Y1 = a^x1 mod q. Signal Y2 may be generated to represent the number obtained by raising the number represented by signal a [sic] to the power represented by signal X2, modulo the number represented by signal q; this transformation may be represented symbolically as Y2 = a^x2 mod q.* col. 4:34-44.

18. As per claim 40, Crandall 5,581,616 discloses within protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and, wherein before transmitting the message M and the digital signature, the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities (see Crandall 5,581,616, Figures 8-12, especially Figure 12; col. 1, lines 50-56), a method by which a receiving unit R that receives the message m and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit R of:

a. retrieving the plurality of public quantities from the publicly accessible repository (see Crandall 5,581,616, col. 1, lines 50-56);

b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two different verification relationships and comparing pairs of results obtained by evaluating the expressions of the at least two different verification relationships (see Crandall 5,581,616, Abstract; Figure 11; col. 20, lines 43-60).

The aforementioned covers claim 40.

19. As per claim 41, Crandall 5,581,616 discloses a method as outlined above in the claim 40 rejection under 35 U.S.C. 103(a). In addition, the plurality of public quantities includes a plurality of vectors by definition of points in n-dimensional coordinate systems used in elliptic curve cryptosystems. See Crandall 5,581,616, col. 6, lines 5-7. The aforementioned covers claim 41.

14. This disclosure does not confine the signal Y1 or Y2 as a single quantity; cryptographic values are commonly identified as vectors containing a plurality of quantities. In fact, Hellman explicitly includes values in m-dimensional space as a set of quantities used in the cryptosystem (col. 8:37-48), i.e. a plurality of quantities. Hence, the prior art of record does teach or suggest all limitations of claim 27.

15. Finally, in reply to applicant's argument that Schneier adds nothing to the disclosure of Hellman et al. (Remarks, pg. 25, 2nd full paragraph), examiner disagrees since an explicit disclosure of a disinterested public repository and the role of the repository clearly teaches the limitation of a public repository for storing public quantities of the cryptographic system and further establishes several objectives as a set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), specifically resolving the level of ordinary skill in the pertinent art and considering objective evidence present in the application indicating obviousness or nonobviousness.

Claim Rejections - 35 USC § 102

16. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

17. Claims 40 and 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Crandall U.S. Patent No. 5,581,616 (hereinafter Crandall 5,581,616).

c. ports (see Hellman, Figure 1, coupling between Reference Nos. 15, 16, 21, 22, 25, 26, 31 and 32):

i. when the cryptographic unit is to receive the ciphertext message M, for:

(1) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit (see Hellman, Figure 1, variables: q, a, Y1 and related text), and the receiving cryptographic unit using the plurality of sender's quantities and at least some of a plurality of public quantities in computing:

(a) at least one receiver's quantity which the receiving cryptographic unit transmits via the communication channel I to the sending cryptographic unit (see Hellman, Figure 1, variable Y2 and related text); and

(b) the key K (see Hellman, Figure 1, variable K within Reference No. 12 and related text); and

ii. when the cryptographic unit is to send the ciphertext message M, for generating the plurality of public quantities (see Hellman, Figure 1, Reference Nos. 21 and 25, and related text), the sending cryptographic unit using the generated plurality of public quantities in computing:

(1) the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the

Claim Rejections - 35 USC § 103

20. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

21. Claims 1-5, 12-18, 25-31, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al. U.S. Patent No. 4,200,770 (hereinafter Hellman) in view of Schneier Applied Cryptography (hereinafter Schneier).

22. As per claim 27, Hellman discloses a cryptographic unit adapted for inclusion in a system for communicating as an encrypted ciphertext message M a plaintext message P that has been encoded using a cryptographic key K (see Hellman, Abstract), the system including:

a. a communication channel I adapted for transmitting the ciphertext message M (see Hellman, Figure 1, Reference No. 19 and variable C); and

b. a pair of transceivers that are coupled to the communication channel I, and that are adapted for communicating the ciphertext message M from one transceiver to the other transceiver via the communication channel I (see Hellman, Figure 1, Reference Nos. 31 and 32);

the cryptographic unit being adapted for coupling to the transceivers for transmitting the ciphertext message M thereto or receiving the ciphertext message M therefrom (see Hellman, Figure 1, Reference Nos. 11 and 12), and comprising:

receiving cryptographic unit (see Hellman, Figure 1, variables q, a, Y1 and related text); and

(2) after receiving via the communication channel I the receiver's quantity from the receiving cryptographic unit, the key K (see Hellman, Figure 1, variable K within Reference No. 11 and related text); and

d. a cryptographic device having:

i. a key input port for receiving the key K from the cryptographic unit (see Hellman, Figure 1, port receiving variable K on device represented as Reference No. 15);

ii. a plaintext port:

(1) for accepting the plaintext message P for encryption into the ciphertext message M that is transmitted from the cryptographic device (see Hellman, Figure 1, port receiving variable P on device represented as Reference No. 15), and

(2) for delivering the plaintext message P obtained by decrypting the ciphertext message M received by the cryptographic device (see Hellman, Figure 1, port delivering variable P on device represented as Reference No. 16); and

iii. a ciphertext port that is coupled to one of the transceivers:

(1) for transmitting the ciphertext message M to such transceiver (see Hellman, Figure 1, port coupling device represented by Reference Nos. 21, 22, 31 and 32), and

(2) for receiving the ciphertext message M from such transceiver (see Hellman, Figure 1, port coupling device representing by Reference Nos. 32 and 22).

23. Hellman does not expressly disclose storing a plurality of public quantities in a publicly accessible repository. However, the variables q and a used in Diffie-Hellman key exchange are public variables within a public-key cryptosystem, which enables these public variables to be published in a public repository as taught by Schneier. See Schneier, page 32, 2nd paragraph; page 515, 'Key Exchange Without Exchanging Keys'. Furthermore, a third party repository acts as a disinterested member of a communications system and can ensure the certification, renewal and cancellation of public information. See Schneier, page 23, 'Arbitrated Protocols'. It would be obvious to one of ordinary skill in the art at the time the invention was made to store the plurality of public quantities in a public accessible repository and retrieve the plurality of public quantities from the public accessible repository for secure key exchange to simplify the key exchange process. See Schneier, page 32, 3rd paragraph. The aforementioned covers claim 27.

24. As per claim 28, Hellman covers a cryptographic unit as outlined above in the claim 27 rejection under 35 U.S.C. 103(a). In addition, Schneier teaches the

cryptographic unit wherein, when receiving the ciphertext message M, in storing the plurality of public quantities into the publicly accessible repository;

a. selects a receiver's secret quantity (see Schneier, page 513, Step 2, 'y');

b. selects for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of selected public quantities (see Schneier, page 513, 2nd paragraph; page 515, 'Key Exchange Without Exchanging Keys'); and

c. using the receiver's secret quantity and the plurality of selected public quantities, computes for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities (see Schneier, page 513, Step 2, 'Y').

25. It would be obvious to one of ordinary skill in the art at the time the invention was made to store a plurality of computed public quantities that are computed using the receiver's secret quantity to enable the Diffie-Hellman key exchange steps as taught by Schneier. Ibid. The aforementioned covers claim 28.

26. As per claims 29-31, Hellman covers a cryptographic unit as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, the plurality of public quantities, the plurality of selected public quantities and the plurality of computed public quantities include a plurality of vectors. See Hellman, col. 8, lines 38-41. The aforementioned cover claims 29-31.

27. As per claim 38, Hellman covers a cryptographic unit as outlined above in the claim 27 rejection under 35 U.S.C. 103(a). In addition, the cryptographic unit wherein, when receiving the ciphertext message M, in computing for transmission to the sending cryptographic unit the at least one receiver's quantity, uses a receiver's secret quantity, at least some of the plurality of public quantities, and at least one of the plurality of sender's quantities received from the sending cryptographic unit. See Hellman, col. 4, line 67. The aforementioned covers claim 38.

28. As per claim 39, Hellman covers a cryptographic unit as outlined above in the claim 38 rejection under 35 U.S.C. 103(a). In addition, the receiver's quantity includes at least one vector. See Hellman, col. 8, lines 38-41. The aforementioned covers claim 39.

29. As per claims 1-5, 12 and 13, they are method claims corresponding to claims 27-31, 38 and 39, and they do not teach or define above the information claimed in claims 27-31, 38 and 39. Therefore, claims 1-5, 12 and 13 are rejected as being unpatentable over Hellman in view of Schneier for the same reasons set forth in the rejections of claims 27-31, 38 and 39.

30. As per claims 14-18, 25 and 26, they are system claims corresponding to claims 27-31, 38 and 39, and they do not teach or define above the information claimed in claims 27-31, 38 and 39. Therefore, claims 14-18, 25 and 26 are rejected as being

unpatentable over Hellman in view of Schneier for the same reasons set forth in the rejections of claims 27-31, 38 and 39.

31. Claims 6-11, 19-24 and 32-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Schneier, and further in view of Crandall U.S. Patent No. 5,159,632 (hereinafter Crandall 5,159,632).

32. As per claim 32, Hellman covers a cryptographic unit as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Hellman does not expressly teach the sending unit selecting a one-time parameter, transmitting it to the receiving unit and using the one-time parameter along with the sender's secret quantity and at least some of the retrieved plurality of public quantities to compute the plurality of sender's quantities. However, in a separate section, Schneier discloses techniques using elliptic curves in the Diffie-Hellman key exchange algorithm. See Schneier, page 480, 6th and 8th paragraphs. As known in the art, elliptic curve systems share coordinate points between the receiver and the sender: this one-time parameter is used to define an elliptic curve group used by the relevant public key cryptosystem. Crandall 5,159,632 teaches such a shared one-time parameter used in an elliptic curve cryptosystem. See Crandall 5,159,632, col. 7, lines 57-60. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Crandall 5,159,632 to the apparatus of Hellman. Motivation for such a combination enables faster public-key

cryptosystems with smaller key sizes as taught by Schneier. Ibid. The aforementioned covers claim 32.

33. As per claim 33, Hellman covers a cryptographic unit as outlined above in the claim 32 rejection under 35 U.S.C. 103(a). In addition, the plurality of sender's quantities includes a plurality of vectors. See Hellman, col. 8, lines 38-41. The aforementioned covers claim 33.

34. As per claims 34-37, they are apparatus claims corresponding to claims 32, 33, 38 and 39, and they do not teach or define above the information claimed in claims 32, 33, 38 and 39. Therefore, claims 34-37 are rejected as being unpatentable over Hellman in view of Schneier and Crandall 5,159,632 for the same reasons set forth in the rejections of claims 32, 33, 38 and 39.

35. As per claims 6-11, they are method claims corresponding to claims 32-37, and they do not teach or define above the information claimed in claims 32-37. Therefore, claims 6-11 are rejected as being unpatentable over Hellman in view of Schneier and Crandall 5,159,632 for the same reasons set forth in the rejections of claims 32-37.

36. As per claims 19-24, they are system claims corresponding to claims 32-37, and they do not teach or define above the information claimed in claims 32-37. Therefore,

claims 19-24 are rejected as being unpatentable over Hellman in view of Schneier and Crandall 5,159,632 for the same reasons set forth in the rejections of claims 32-37.

Conclusion

37. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
March 21, 2005

Gilberto B

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100